MC-WR11
MC-WR22

Wireless router



user's manual

MODECOM

Contents

User's manual guide

GB

Latest versions of manuals, quick start guides, drivers and software are available on www.modecom.eu website.

IMPORTANT NOTE:

Provided technical specifications are subject to change without prior notice. All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Chapter 1 Introduction

Congratulations on your purchase of this outstanding Wireless Router. The Wireless Router integrates 4-port switch, firewall, NAT-router and Wireless Access Point. This product is specifically designed for Home networks and Medium or Small Corporation needs. It will allow you to connect your network wirelessly better than ever, sharing Internet Access, files and fun, easily and securely. It is easy to configure and operate even for users without wide experience with network devices. Instructions for installing and configuring this product can be found the manual delivered with the product and also available at www.modecom.eu website. Before you install and use this product, please read this manual carefully to exploit all the functions of this product.

Features

WAN: Gateway / Bridge / WISP / Static IP / DHCP / PPPoE / PPTP / L2TP / UPnP

LAN: RJ45 4port switch / DHCP Client, Server / Static DHCP / IP&MAC Bind

Wireless: Compliant with draft IEEE 802.11n standard (MC-WR22- 2T2R / MC-WR11 – 1T1R)

Up to: 300Mbps (MC-WR22) / 150Mbps (MC-WR11) data transfer rates in IEEE 802.11n mode

Backward compatible with IEEE 802.11b/g

Supports both Infrastructure and Ad-Hoc Networking Modes

Work modes: AP / Client / WDS / AP+WDS / Universal Repeater (AP+Client)

Supports WPS, WPA2 (802.11i), WPA, WPA2/WPA Mixed, 802.1x advanced security

Supports 64/128-bit WEP Data Encryption

Quality of Service (QoS) - WMM, WMM-PS
Auto wireless transmission channel select for optimal performance
Wireless access control (MAC address filter)

Advanced Wireless control:
Fragment Threshold / RTS Threshold / Beacon Interval
Preamble Type: Long / Short
IAPP - Roaming (802.11f)
Protection / Aggregation / Short GI / WLAN Partition
RF Output Power control
Multiple BSSID

Dynamic DNS:
DynDNS.org / TZO / 3322.org

NAT:
NAT/NAPT IP sharing / DMZ / Port Forwarding / Port Trigger / UPnP

QoS:
Yes - IP (single or range) Grant MIN or MAX bandwidth

Firewall protection:
Ping Access on WAN / IGMP Proxy / Web Server Access on WAN / IPsec/ PPTP/L2TP VNP pass through /
Src MAC or IP Filter / URL Filter / Dst IP and Port Filter /

DoS Prevention:
Whole System Flood: SYN, FIN, UDP, ICMP
Per-Source IP Flood: SYN, FIN, UDP, ICMP
TCP/UDP Port Scan (High/Low Sensitivity)
ICMP Smurf, IP Land, IP Spoof, IP TearDrop, PingOfDeath, TCP Scan, TCP SynWithData, UDP Bomb, UDP EchoChargen
Source IP Blocking (Block for a specified time)

System Management:
Access Schedule / NTP support / FW Upgrade / Save/Load Config / Reboot / User name and password management

1.2 Operation Environment

Dimensions: 202 (L) x 120 (W) x 31 (H)mm
Unit Weight: 324g
Power Input: 9V DC, 1A
Consumption: 13.5W(Max)
Storage Temperature: -40ºC ~70ºC

Operating Temperature : -10ºC ~50ºC
Storage Humidity: 5% ~95% RH Non-condensing
Operating Humidity: 10% ~90% RH Non-condensing

1.3 System Requirements

An Ethernet-Based Cable or DSL modem
10/100M Ethernet Card on PC
TCP/IP network protocol for each PC
RJ45 Twisted-pair cable
Internet browser: Microsoft Internet Explorer, Firefox, Opera or Chrome

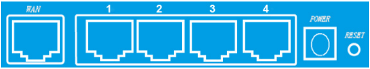
Chapter 2 Hardware Installation

2.1 Led indicators



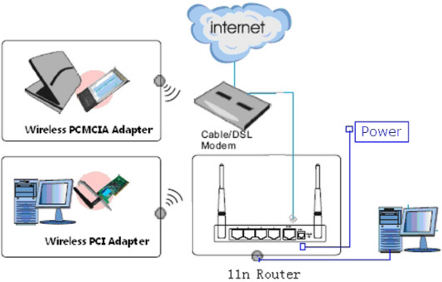
SYS/Power (Red): Flickering light indicates a proper connection to the power supply.
While resetting the SYS LED will flash differently (shine for 2 seconds and stop for 1 second).
WPS (Green): The Led will flicker for about two minutes when WPS session is active .
WLAN (Wireless LAN) (green): The LED is flickering during wireless activity.
LAN 1,2,3,4 (green): The Link/Act LED serves two purposes. If the LED is continuously illuminated, the Router is successfully connected to a device through the corresponding port. If the LED is flickering, the Router is actively sending or receiving data over that port.
WAN (Green): The Link/Act LED serves two purposes. If the LED is continuously illuminated, the Router is successfully connected to a device through the corresponding port. If the LED is flickering, the Router is actively sending or receiving data over that port.

2.2 Back Panel Features



LAN(1,2,3,4): 10/100Mbps RJ45 Auto-sensing. These four LAN ports are where you will connect other network devices, such as PCs/Laptops, print servers, remote hard drives, and anything else you want to put on your network. If you connect this product with the Network adapter, Hub (or Switch) correctly, the Router's corresponding LED and the Adapter's, Hub's (or the Switch) will illuminate.
WAN: 10/100Mbps RJ45 port. The WAN port is where you will connect Cable/DSL Modem or other LAN.
RESET(WPS): The Reset Button has three functions, WPS, reboot and Factory Default. When press it less than 2 second, it is WPS function and the SYS LED will flash two minute (as long as WPS session is active); 2 to 5 seconds, the router will reboot; and more than 5 seconds, the router will restore to factory default settings.
Power inlet: 9V DC, 1A Power supply.

2.3 Typical install



1. Make sure all devices, including your PCs, modem, and Router, are turned on.
2. Using an Ethernet network cable, connect the LAN device or Ethernet network port of the cable or DSL modem to the Router's WAN port.

Chapter 3 Quick Install Guide

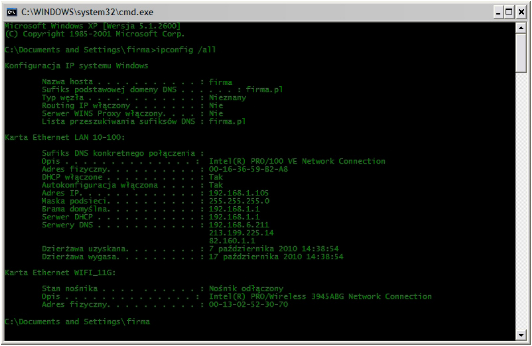
3.1 TCP/IP Settings

Before you can access and configure router, you have to setup your network adapter IP address. According to the following steps to obtain IP address automatically from router DHCP Server, The following instruction set up the computer running windows operation system.

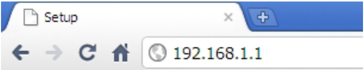
Note: The router default IP address is 192.168.1.1

1. Click Start button and choose Settings, then click Control Panel.
2. Double click Network icon and select Configuration tab in the Network window.
3. Choose the connection you want to use and click it with right mouse button and choose “Properties”.
4. Double click TCP/IP Protocol.
5. Make sure that option “Obtain IP address automatically” is chosen.
8. Click OK to complete the install procedure.

After all is successful, you can check the TCP/IP information via the following command. Start -> run. Type cmd and in the window like the one below enter command: ipconfig /all.

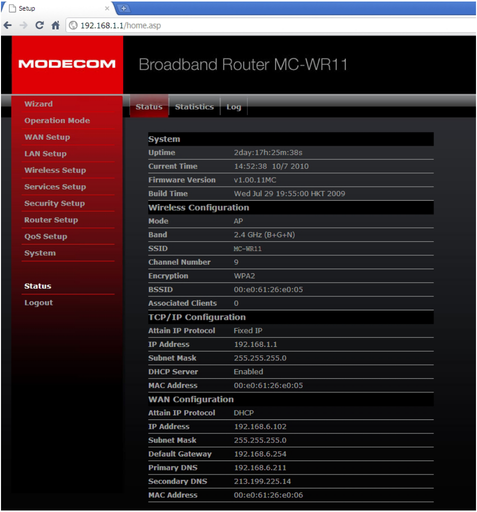


3.2 Getting Started



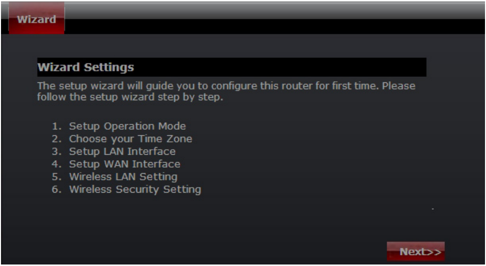
To access configuration panel open your web browser (MS Internet Explorer, Firefox, Opera or Chrome) and type the router's IP address: 192.168.1.1
Default User / Password: admin

If successful, you can see the status page.



3.3 Setup Wizard

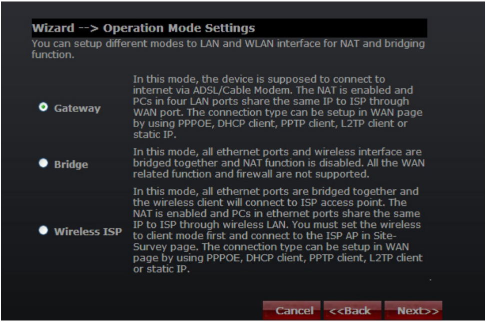
Click on “Wizard”, it will guide you to setup your router in six simple steps.



Please follow the steps and complete the router configuration.

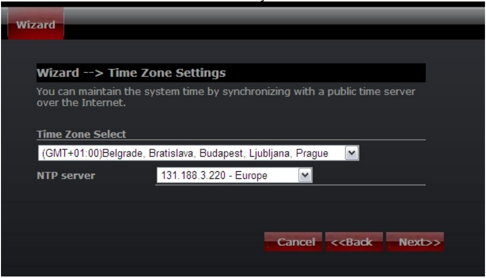
Step 1 - Setup Operation Mode

The router supports three operation modes, Gateway, Bridge and Wireless ISP. And each mode is suitable for different use, please choose correct mode.



Step 2 - Time Zone Settings

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock.

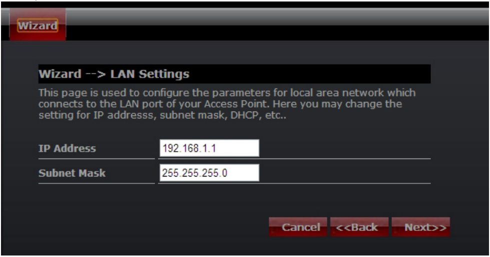


Time Zone Select: Select the Time Zone from the drop-down menu.

NTP Server: Select the NTP Server from the drop-down menu.

Step 3 - LAN Settings

Setup the IP address and Subnet mask for the LAN interface.

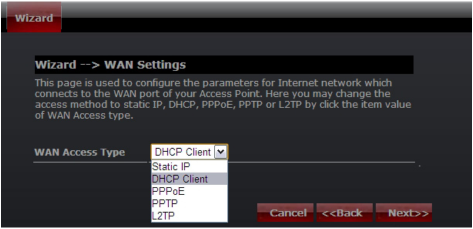


Step 4 - WAN Settings

The Router support five access modes in the WAN side, please choose correct mode according to your ISP Service.

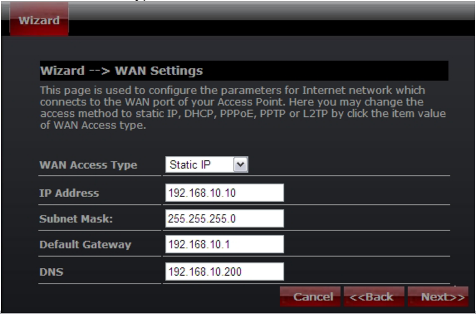
Mode 1: DHCP Client

Select DHCP Client to obtain IP Address information automatically from your ISP. This mode is commonly used for Cable modem services.

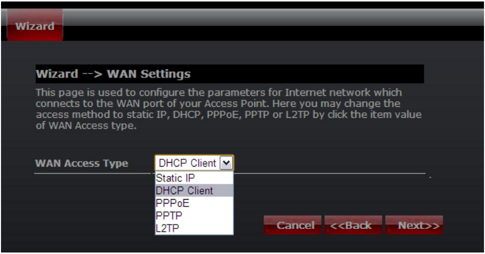


Mode 2: Static IP

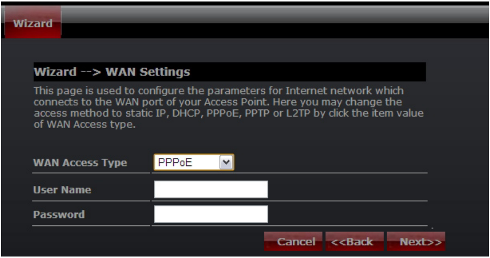
Select Static IP Address if all IP information is provided to you by your ISP. You will need to enter in the IP address, subnet mask, gateway address, and DNS address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four numbers (from 0 to 255) separated by dots (x.x.x.x). The Router will not accept the IP address if it is not typed in this format.



IP Address: Enter the IP address assigned by your ISP
Subnet Mask: Enter the Subnet Mask assigned by your ISP.
Default Gateway: Enter the Gateway assigned by your ISP.
DNS: Enter the DNS server assigned by your ISP.

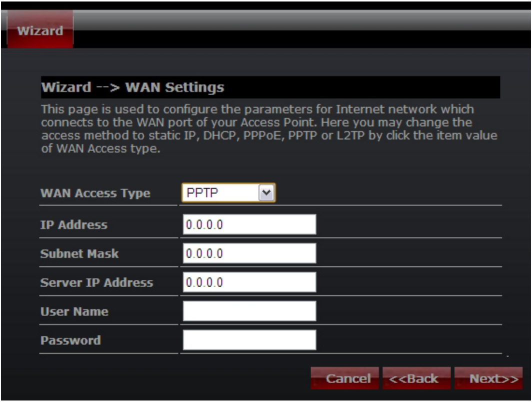


Mode 3: PPPoE
Choose PPPoE (Point to Point Protocol over Ethernet) if your ISP uses a PPPoE connection. Your ISP will provide you with a username and password.



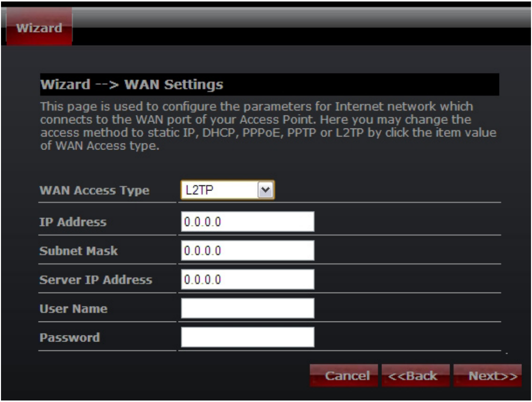
User Name: Enter your PPPoE user name.
Password: Enter your PPPoE password.

Mode 4: PPTP
Choose PPTP (Point-to-Point-Tunneling Protocol) if your ISP uses a PPTP connection. Your ISP will provide you with IP information and PPTP Server IP Address, of course it also includes a username and password.



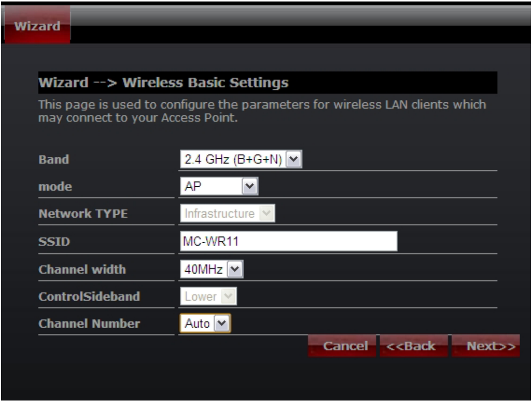
IP Address: Enter the IP address.
Subnet Mask: Enter the subnet Mask.
Server IP Address: Enter the PPTP Server IP address provided by your ISP.
User Name: Enter your PPTP username.
Password: Enter your PPTP password.

Mode 5: L2TP
Choose L2TP (Layer 2 Tunneling Protocol) if your ISP uses a L2TP connection. Your ISP should provide you with a username, password and all necessary data.



IP Address: Enter the IP address.
Subnet Mask: Enter the subnet Mask.
Server IP Address: Enter the PPTP Server IP address provided by your ISP.
User Name: Enter your PPTP username.
Password: Enter your PPTP password.

Step 5: WLAN Settings
Wireless Interface: If you do not want to use wireless, uncheck the box to disable all the wireless connections.

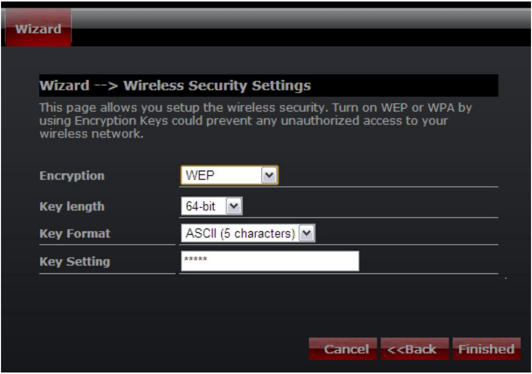


Band: Supported standards: 802.11B, 802.11G, 802.11N and mixed. Please choose its band according to standards used by devices which will be connected to router.
Mode: Support AP, Client, WDS and AP+WDS mode.
Network TYPE: This type is only valid in client mode.
SSID: Service Set Identifier, it identifies your wireless network.
Channel width: Select 40MHz if you use 802.11n or 802.11n mixed mode, otherwise 20MHz, it is default value.
Control Sideband: it is only valid when you choose channel width 40MHz.
Channel Number: Indicates the channel setting for the router. By default the channel is set to 6.

Step 5: WLAN Security Settings

Secure your wireless network by turning on the WPA or WEP security feature on the router. This section you can set WEP, WPA, WPA2 and mixed security mode.

The following picture shows how to set the WEP security.



Key length: WEP supports 64-bit or 128-bit security key.
Key Format: User can enter key in ASCII or Hex format.
Key Setting: Enter the key, accordingly to chosen format.

The keys are used to encryption data transmitted in the wireless network. Fill in the text box by following rules below:

• 64-bit: Input any 5 ASCII characters or 10 digit Hex values (in the "A-F", "a-f", and
"0-9" range) as the encryption keys. It is advised to use digits and both low-ercase and uppercase characters - for example: "012345aEfG"

• 128-bit: Input any 13 ASCII characters or 26 digit Hex values (in the "A-F", "a-f", and "0-9" range) as the encryption keys. For example: 01234567890123456789aBcDEf"

The following picture shows how to set WPA-PSK security, you can select WPA(TKIP), WPA2(AES) and Mixed mode.



Pre-Shared Key Format: Specify the format of the key, passphrase or hex.
Pre-Shared Key: Enter the key, accordingly to chosen format.

The keys are used to encryption data transmitted in the wireless network. Fill in the text box by following rules below:

• 64-bit: Input any 5 ASCII characters or 10 digit Hex values (in the “A-F”, “a-f”, and
“0-9” range) as the encryption keys. It is advised to use digits and both lowercase and uppercase characters - for example: “012345aEfG”

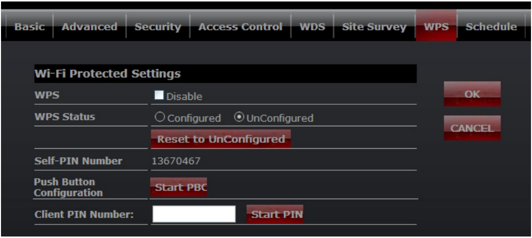
• 128-bit: Input any 13 ASCII characters or 26 digit Hex values (in the “A-F”, “a-f”, and “0-9” range) as the encryption keys. For example: 01234567890123456789aBcDEf”

Chapter 4 Advanced Setup

4.1 Wireless Advanced setup

4.1.1 WPS

WPS is designed to ease set up of security Wi-Fi networks and subsequently network management. This router supports WPS features for AP mode, AP+WDS mode, Infrastructure-Client mode, and Universal Repeater mode.



WPS: Checking this box and clicking “OK” will disable WPS function. WPS is turned on by default.

WPS Status: When Router’s settings are factory default, it is set to open security and un-configured state, some registers such as Vista WCN can configure AP. Otherwise If it already shows “Configured”, it means that the router has setup its security.

Self-PIN Number: Its is AP’s PIN.

Start PBC: Clicking this button will invoke the Push Button Configuration of WPS. If one station wants to connect to the AP, you must click its PBC button within two minutes. You can see the WPS led flash this time.

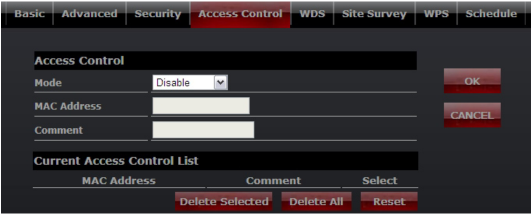
Note: This router also has a hardware button, it is same button with reset. When press this button for less than two seconds, the AP will run PBC function and the reset LED will flash for two minutes, during WPS session. The station can connect to the AP by its software or hardware WPS button.

Please also note – If you press and hold this button 2 to 5 seconds, the router will reboot; more than 5 seconds, the router will restore factory default.

Client PIN Number: The length of PIN is limited to four or eight numeric digits. If the AP and Station have the same PIN number typed in and clicked “Start PIN” button within two minutes, they will establish connection and setup their security key.

4.1.2 Access Control

The Wireless MAC Address Filtering feature allows you to control wireless stations accessing the router, depending on their MAC addresses.



Mode: If you choose '**Allow Listed**', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When **'Deny Listed'** is selected, these wireless clients on the list will not be able to connect the Access Point. The MAC Address format is 001122334455.

4.1.3 Wireless Distribution System (WDS)

WDS uses wireless media to communicate with other APs, like the Ethernet does. To do this, firstly you must set AP Mode to WDS or AP+WDS in basic setting, then enable WDS function and set another AP MAC which you want to communicate with. The WDS supports WEP and WPA security mode. Of course in order to make APs work, you have to keep them working on the same channel and security mode as source AP.

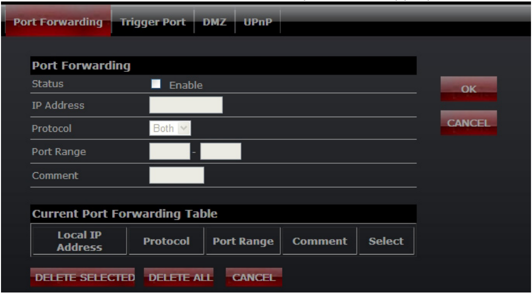


WDS: Check this box to enable WDS function.
MAC Address: Enter the remote AP MAC address.
Security: Set WDS security.
Encryption: You may select WEP 64bits, WEP 128bits, WPA (TKIP), WPA (AES).
WEP Key Format: You may select to select ASCII Characters or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the WEP Key.
WEP Key: Set key to encrypt your data
Pre-Shared Key Format: You can select PASSPHRASE or HEX(64 CHARACTERS).
Pre-Shared Key: Enter the key accordingly to chosen format.

4.2 Service Setup

4.2.1 Port Forwarding

If you configure the router as Virtual Server, remote users accessing services such as Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP address. In other words, depending on the requested service (TCP/UDP port number), the router redirects the external service request to the appropriate server.

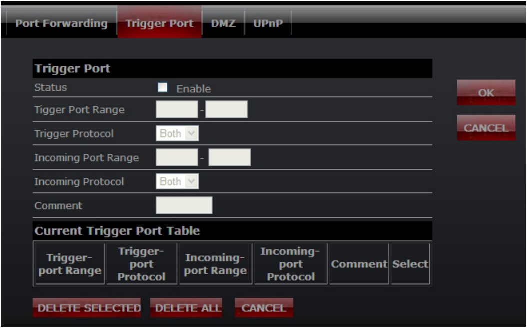


Status: Clicking this box will enable Port Forwarding function.
IP Address: Local IP to which the request from external user will be redirected.

Protocol & Port Range: The packet with this protocol and port will be re-directed to their local IP.
Comment: You can add some comment for this item.
Current Filter Table: The table shows all you have configured. You can delete one or all.

4.2.2 Trigger Port

Some applications require multiple connections, like Internet games, video conferencing and so on. These applications cannot work with a pure NAT router. Trigger Port function allows router to open an incoming port for traffic and close it when it is unused. When the traffic is outgoing the router will expect the answer from remote server and the specific the port will be open.

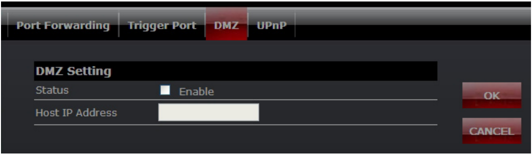


Status: Check on to enable this function.
Trigger Port Range: The port for outgoing traffic. An outgoing connection using this port will “”Trigger” this rule.
Trigger Protocol: The protocol used for Trigger Ports, either TCP, UDP or Both.
Incoming Port Range: The port or port range used by the remote system when it responds to the outgoing request. A response using one of the these ports will be forwarded to the PC that triggered the rule.

Incoming Protocol: The Protocol used for Incoming Ports Ranges, either TCP or UDP, or both.
Comment: You can add some comment for this item.

4.2.3 Demilitarized Zone (DMZ)

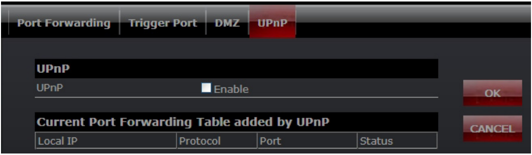
If you have a client PC that cannot run Internet application properly from behind the NAT firewall or after configuring the Port Forwarding, then you can open the client up to unrestricted two-way Internet access.



Status: Clicking this box will enable DMZ function.
Host IP Address: Enter DMZ host IP Address may expose this host to a variety of security risks.

4.2.4 Universal Plug and Play (UPNP)

UPnP feature allows the devices to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.



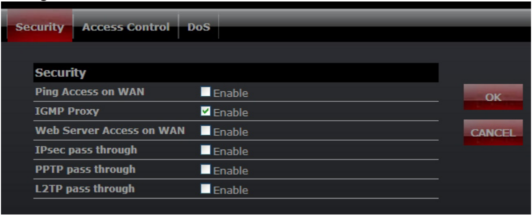
UPnP: Check on to enable UPnP function
Note: The pages also list the forwarding port added by UPnP Service.

4.3 Security Setup

The router provides extensive firewall protection by restricting connection parameters to limit the risk of intrusion and defending against a wide array of common hacker attacks.

4.3.1 Security

The firewall will allow or block some services according to the following settings.



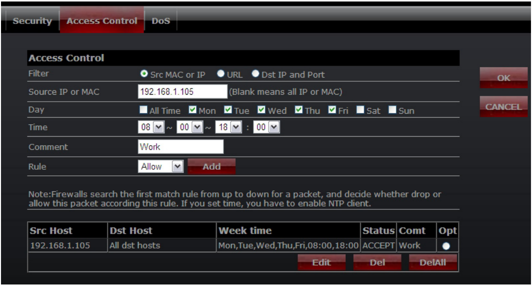
Ping Access on WAN: Whether allow or block to Ping WAN interface.
IGMP Proxy: Simple, dynamic Multicast Routing Daemon using only IGMP signaling. It's used for simple forwarding of Multicast traffic between networks.
Web Server Access on WAN: Whether allow or not to access Web Server from WAN interface.
VPN pass through: Whether to allow Virtual Private Network (VPN) connections.

4.3.2 Access Control

In this section you can set up some rules, for example MAC filter, IP filter, URL filter and Port filter. You also can add extra control on these rules according to the date and time, but you must enable NTP client first.
Note 1: When one packet arrives, firewall will search this rules table from up to down and stop if it find match one. Then the packet will be forward or drop according to the rule. If none is matched, the firewall will allow it pass.
Note 2: Click "Add" button to add this rule to table and click "OK" to apply to router and take effective. You also can edit or del some one

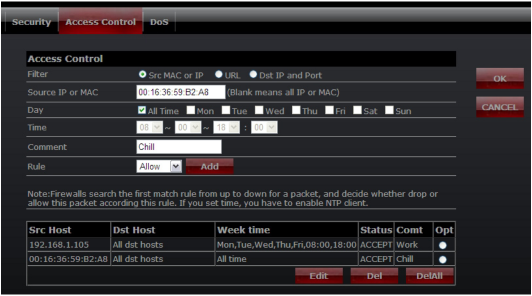
1. IP Filter

Allow or block the computers according to its IP address.



2. MAC filter

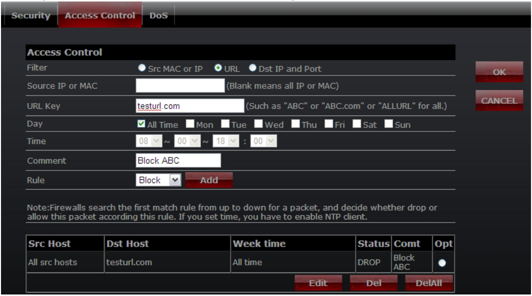
Allow or block the computers according to its MAC address.



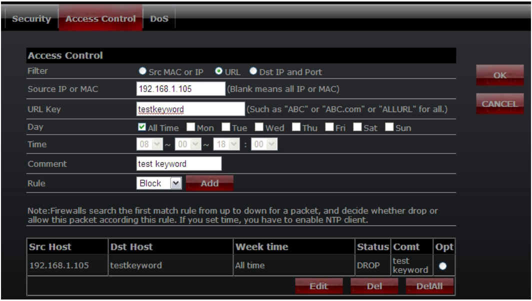
3. URL filter

You can block some URL according to URL Key words. If Source IP or MAC is blank, it means all computers can not access this URL, otherwise the rule will be only valid to one computer with this IP or MAC address.

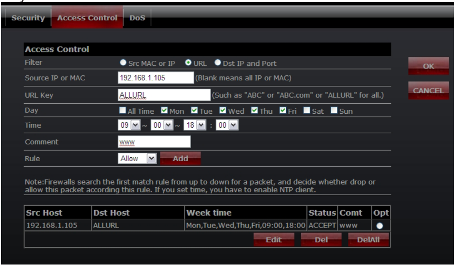
Example 1: Block “testurl.com” at all computers.



Example 2: Block all URL with “testkeword” at one computer with IP address 192.168.1.105.

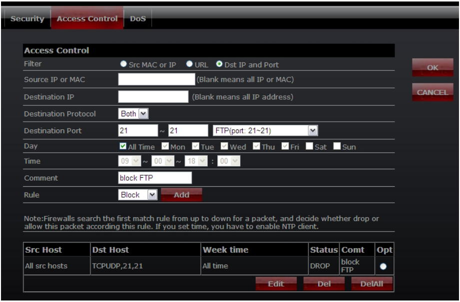


Example 3: Block all URL at all computers from 09:00 to 18:00 on working days.

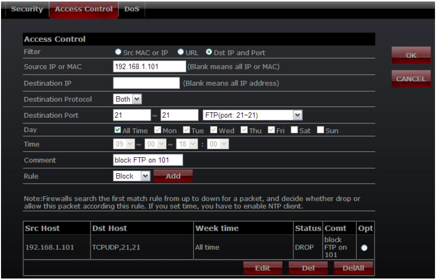


4. Port filter

You can limit some or all computers to access some destination IP and port.
Example 1, block all computer to access port 21.

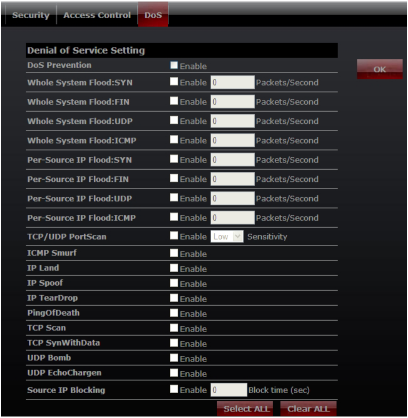


Example 2, block one computer with IP address 192.168.1.101 to access port 21.



4.3.3 Denial of Service (DoS)

This page used to Block DoS attack.



4.4 QoS Setup

The QoS helps improve your network gaming performance by prioritizing applications. By default the bandwidth control is disabled and application priority is not classified automatically.

In order to complete this settings, Please follow the steps below.

Enable this function.

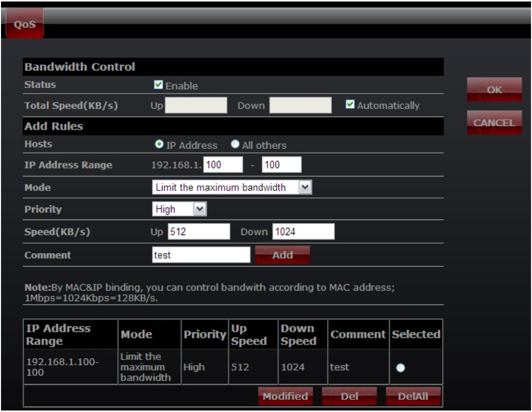
Enter the total speed or choose automatic mode.

Enter the IP address user want to control.

specify how to control this PC with this IP address, include Maximum or minimum bandwidth, priority and its up/down speed.

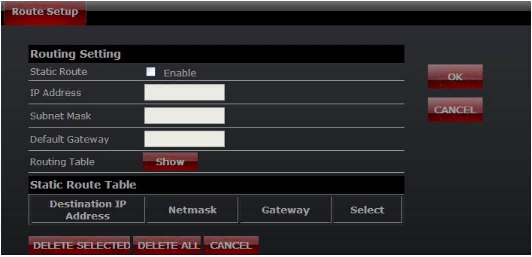
Click Add button to add this item to control table

Clicks OK button to apply these rules.



4.5 Router Setup

A static route is a pre-determined pathway that data packets must travel to reach a specific host or network.



Static Route: Click this box to enable static route.
IP Address: The network or host IP address desired to access.
Subnet Mask: The subnet mask of destination IP.
Default Gateway: The gateway is the router or host's IP address to which packet was sent. It must be the same network segment with the WAN or LAN port.
Routing Table: Clicking this button will show you all the routing table of the system.
Static Routing table: It only shows the static routing table and you can delete one or all.

4.6 System

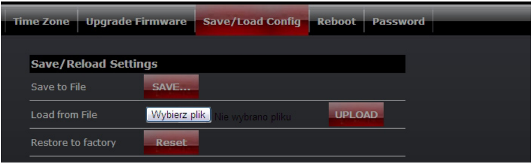
4.6.1 Upgrade Firmware

You can upgrade Firmware in this page.



4.6.2 Save/Load Config

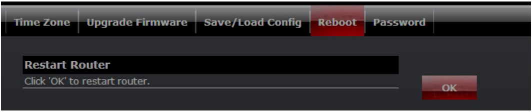
You can backup or restore the system configuration in this page.



Save to File: Save the router's settings and store it in your local computer.
Load from File: Restore the settings from saved file.
Resotore to factory: Restore the system settings to factory default.

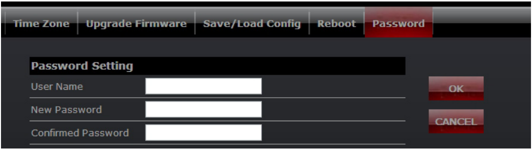
4.6.3 Reboot

You can reboot device via clicking the Reboot button.



4.6.4 Password

To ensure the Router's security, you will be asked for user name and password when you access the Router's Web-based config panel. **The default user name and password is: admin / admin**.
This page will allow you to modify the User name and password.



Spis treści

Instrukcja instalacji

PL

Najnowsze wersje instrukcji, sterowników i oprogramowania dostępne są na stronie www.modecom.pl

WAŻNA INFORMACJA: Podane dane techniczne mogą ulec zmianie bez wcześniejszego powiadomienia. Wszystkie znaki towarowe umieszczone w instrukcji należą do ich właścicieli.

Rozdział 1 - Wprowadzenie

Gratulujemy zakupu tego wspaniałego routera. Bezprzewodowy Router MC-WR22 / MC-WR11 łączy 4-portowy przełącznik, zaporę ogniową, router NAT i punkt dostępowy sieci bezprzewodowej. Ten produkt został zaprojektowany specjalnie dla potrzeb sieci domowych oraz małych i średnich przedsiębiorstw. Pozwala na łatwe i bezpieczne podłączenie do sieci innych urządzeń zarówno bezprzewodowo jak i tradycyjnymi kablami Ethernetowymi. Jest łatwy w konfiguracji i obsłudze nawet dla użytkowników bez szerokiego doświadczenia w tym zakresie. Informacje dotyczące instalacji i konfiguracji tego produktu można znaleźć w instrukcji obsługi dostarczonej razem z produktem oraz dostępnej na stronie www.modecom.pl. Przed instalacją i używaniem produktu, należy uważnie przeczytać instrukcję by móc w pełni korzystać ze wszystkich jego funkcji.

1.1 Specyfikacja

WAN: Brama (Gateway) / Most (Bridge) / WISP / Statyczny adres IP / DHCP / PPPoE / PPTP / L2TP / UPnP

LAN: 4portowy przełącznik RJ45 / DHCP klient, serwer / Rezerwacja adresów w DHCP / Przypisywanie adresów IP do MAC

Wireless: Wsparcie dla standardu IEEE 802.11n (MC-WR22 - 2T2R / MC-WR11 – 1T1R)

Prędkość transmisji: MC-WR22 do 300Mbps / MC-WR11 do 150Mbps

Wsteczna zgodność ze standardami IEEE 802.11b/g

Wsparcie trybów Infrastructure i Ad-Hoc

Tryby pracy: Punkt dostępowy (AP) / klient / WDS / AP+WDS / Universal Repeater (AP+Client)

Zaawansowane szyfrowanie: WPS; WPA2 (802.11i), WPA, WPA2/WPA tryb mieszany, 802.11x

Szyfrowanie 64/128-bit WEP
Obsługa Quality of Service (QoS) - WMM, WMM-PS
Automatyczny wybór optymalnego kanału transmisji bezprzewodowej
Kontrola dostępu do sieci bezprzewodowej (filtr adresów MAC)
Zaawansowane ustawienia sieci bezprzewodowych:
Próg fragmentacji / Próg mechanizmu RTS / Częstotliwość wysyłania Beacon
Długość Preambuły (długa / krótka)
Roaming - IAPP (802.11f)
Regulacja mocy nadajnika
Multiple BSSID
Dynamic DNS: DynDNS.org / TZO / 3322.org
NAT: NAT/NAPT współdzielenie IP / Strefa zdemilitaryzowana (DMZ) / Przekierowanie portów (Port Forwarding) / Wyzwalanie portów (Port Trigger) / UPnP
QoS: Tak - dla IP (pojedynczy lub zakres) Przydzielenie MIN lub MAX przepustowości
Zapora Firewall: Ping Access on WAN / IGMP Proxy / Web Server Access on WAN / IPsec/PPTP/L2TP VNP pass through / Filtr IP lub MAC / Flirt adresów URL / Filtr źródłowych adresów IP I portów.
Ochrona przed atakami typu DoS:
Whole System Flood: SYN, FIN, UDP, ICMP
Per-Source IP Flood: SYN, FIN, UDP, ICMP
TCP/UDP PortScan (High/Low Sensitivity)
ICMP Smurf, IP Land, IP Spoof, IP TearDrop, PingOfDeath, TCP Scan, TCP SynWithData, UDP Bomb, UDP EchoChargen
Blokowanie adresu IP (przez określony czas)
Zarządzanie:
Harmonogram dostępu / synchronizacja czasu z serwerami NTP / Aktualizacja oprogramowania / Zapisywanie/Przywracanie konfiguracji

1.2 Środowisko pracy

Wymiary: 202 (dł.) x 120 (szer.) x 31 (wys.) mm; Waga: 324g
Zasilanie: 9V DC, 1A
Pobór mocy: 13.5W (max)
Temperatura otoczenia podczas pracy: -10 º C ~ 50 º C
Temperatura otoczenia podczas przechowywania: -40 º C ~ 70 º C
Wilgotność otoczenia podczas pracy urządzenia: 5% ~ 95% RH (bez kondensacji)

Wilgotność otoczenia podczas przechowywania urządzenia: 10% ~ 90% RH (bez kondensacji)

1.3 Wymagania systemowe

Połączenie Ethernet lub modem DSL
Karta Ethernet na PC 10/100M
Obsługa protokołu TCP / IP dla każdego komputera
Kabel Ethernet RJ45
Przeglądarka internetowa Microsoft Internet Explorer, Firefox, Opera lub Chrome

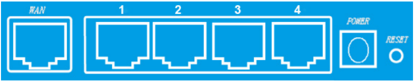
Rozdział 2 - Instalacja

2.1 Diody LED



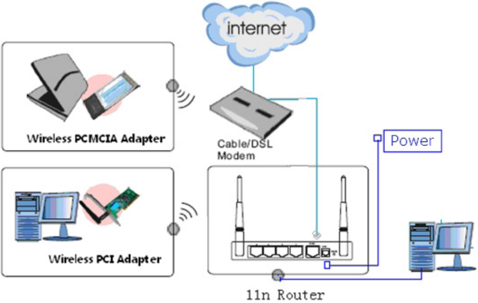
SYS / Power (czerwona): Dioda miga, gdy urządzenie jest podłączone do zasilania.
Podczas resetowania urządzenia dioda miga w innym rytmie (zapala się na ok. 2 i gaśnie na ok. 1 sekundę)
WPS (zielona): Dioda miga przez około 2 minuty podczas trwania sesji WPS.
WLAN (zielona): Dioda miga podczas komunikacji bezprzewodowej.
LAN 1,2,3,4 (zielone): Link/Act LED służy dwóm celom. Jeśli dioda świeci ciągle, router jest z prawidłowo podłączony do urządzenia za pomocą odpowiedniego portu. Jeśli dioda, która jest przypisana do danego portu miga, router jest w trakcie wysyłania lub/i odbierania danych przez ten port.
WAN (zielona): Dioda Link/Act służy dwóm celom. Jeśli dioda świeci ciągle, router jest z prawidłowo podłączony do urządzenia za pomocą odpowiedniego portu. Jeśli dioda, która jest przypisana do danego portu miga, router jest w trakcie wysyłania lub/i odbierania danych przez ten port.

2.2 Panel tylny urządzenia



LAN (1,2,3,4): RJ45 10/100Mbps. Do tych czterech portów LAN, można podłączyć urządzenia sieciowe, takie jak komputery PC/Laptopy, serwery wydruku, zewnętrzne dyski twarde i wszystko, co chcesz podłączyć do sieci. Jeśli router jest poprawnie połączony z kartą sieciową, Hubem (lub przełącznikiem), diody na routerze i Hubie (lub przełączniku) będą świecić.
WAN: 10/100 Mbps port RJ45. Port WAN do którego należy podłączyć model kablowy DSL lub inne urządzenie sieci LAN.
RESET (WPS): Przycisk „Reset" ma trzy funkcje: WPS, restart i przywracanie ustawień fabrycznych. Po naciśnięciu go na mniej niż 2 sekundy, uruchamiana jest sesja WPS i dioda SYS miga przez ok. 2 minuty (czas trwania sesji WPS). Przytrzymanie przycisku od 2 do 5 sekund spowoduje restart routera. Przytrzymanie go dłużej niż 5 sekund spowoduje przywrócenie urządzenia do ustawień fabrycznych.
Gniazdo zasilania: Zasilacz 9V DC, 1A

2.3 Typowa instalacja



1. Sprawdź, czy wszystkie urządzenia, w tym komputery PC, modem i router, są wyłączone.
2. Korzystając z kabla sieciowego Ethernet podłączyć modem kablowy lub inne urządzenie LAN do portu WAN routera.

Rozdział 3 - Skrócona instrukcja instalacji

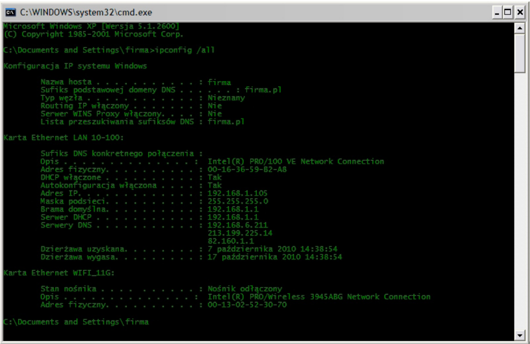
3.1 Ustawienia TCP / IP

Aby uzyskać dostęp do panelu konfiguracyjnego routera, należy skonfigurować kartę sieciową. Postępuj zgodnie z instrukcją w celu uzyskania adresu IP automatycznie z serwera DHCP routera, Poniższa instrukcja opisuje konfigurowanie komputera z systemem operacyjnym Windows.

Uwaga: domyślny adres IP routera to 192.168.1.1.

1. Kliknij przycisk „Menu Start" i wybierz „Ustawienia", a następnie kliknij polecenie „Panel sterowania".
2. Kliknij dwukrotnie ikonę „Połączenia Sieciowe".
3. Wybierz połączenie, którego chcesz użyć i kliknij na nie prawym przyciskiem myszy, następnie wybierz „Właściwości".
4. Kliknij dwukrotnie, „Protokół TCP / IP".
5. Upewnij się, że wybrana jest opcja automatycznego uzyskiwania adresu IP.
6. Kliknij przycisk OK, aby zakończyć procedurę instalacji.

Gdy protokół TCP/IP jest skonfigurowany poprawnie można wyświetlić informacje na jego temat za pomocą
następującego polecenia: Menu Start > Uruchom - wpisz polecenie: cmd; W oknie takim jak poniżej wpisz polecenie: ipconfig / all i naciśnij Enter.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Wersja 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\firma>ipconfig /all

Konfiguracja IP systemu Windows

        Nazwa hosta . . . . . . . . . . . . . : firma
        Sufiks podstawowej domeny DNS . . . . . . . : firma.pl
        Typ węzła . . . . . . . . . . . . . . : Nieznany
        Routing IP włączony . . . . . . . . . : Nie
        Serwer WINS Proxy włączony. . . . . : Nie
        Lista przeszukiwania sufiksów DNS : firma.pl

Karta Ethernet LAN 10-100:

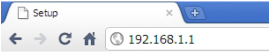
        Sufiks DNS konkretnego połączenia :
        Opis . . . . . . . . . . . . . . . . :  Intel(R) PRO/100 VE Network Connection
        Adres fizyczny. . . . . . . . . . . . : 00-16-36-59-B2-A8
        DHCP włączone . . . . . . . . . . . . : Tak
        Autokonfiguracja włączona . . . . . : Tak
        Adres IP. . . . . . . . . . . . . . . : 192.168.1.105
        Maska podsieci. . . . . . . . . . . . : 255.255.255.0
        Brama domyślna. . . . . . . . . . . . : 192.168.1.1
        Serwer DHCP . . . . . . . . . . . . . : 192.168.1.1
        Serwery DNS . . . . . . . . . . . . . : 192.168.6.211
                                                213.199.225.14
                                                82.160.1.1
        Dzierżawa uzyskana. . . . . . . . . . : 7 października 2010 14:38:54
        Dzierżawa wygasa. . . . . . . . . . . : 17 października 2010 14:38:54

Karta Ethernet WIFI_11G:

        Stan nośnika . . . . . . . . . . . . : Nośnik odłączony
        Opis . . . . . . . . . . . . . . . . :  Intel(R) PRO/Wireless 3945ABG Network Connection
        Adres fizyczny. . . . . . . . . . . . : 00-13-02-52-30-70

C:\Documents and Settings\firma
```

3.2 Wprowadzenie



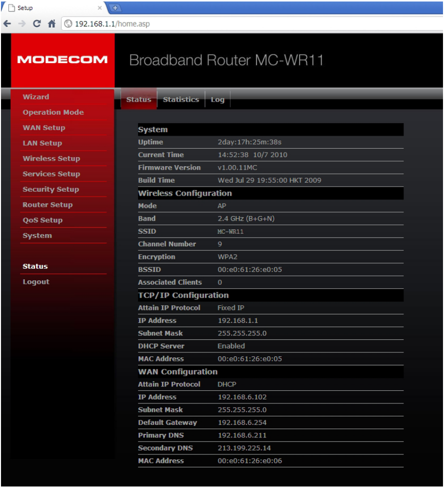
Aby uzyskać dostęp do panelu konfiguracyjnego, należy otworzyć przeglądarkę internetową, taką jak Internet Explorer / Firefox / Opera / Chrome i wpisać adres IP routera: 192.168.1.1

Domyślne parametry logowania:

nazwa użytkownika: admin

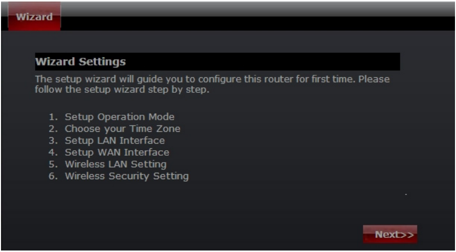
hasło: admin

Jeśli połączenie jest ustanowione i logowanie się powiedzie w przeglądarce ukaże się strona z danymi na temat stanu urządzenia



3.3 Kreator konfiguracji (Setup Wizard)

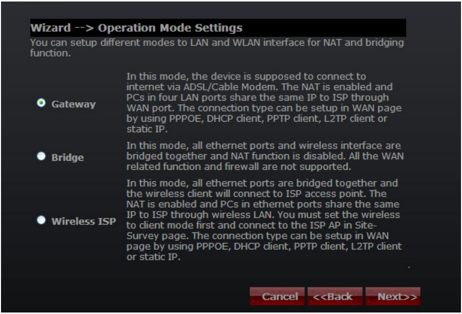
Aby uruchomić kreator, który przeprowadzi cię krok po kroku przez proces konfiguracji kliknij na „Wizard”. Kreator podzielony jest na sześć etapów.



Postępuj zgodnie z poleceniami by przeprowadzić konfigurację routera.

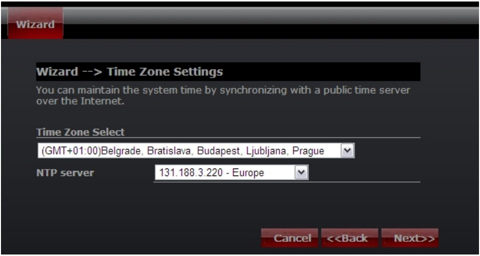
Krok 1 - Tryb pracy

Router obsługuje trzy tryby pracy: Gateway (brama), Bridge (most), oraz Wireless ISP (bezprzewodowy dostawca Internetu). Każdy tryb jest przygotowany dla innego zastosowania, należy wybrać właściwy tryb.



Krok 2 - Ustawienia strefy czasowej

Ustawienia serwera czasu umożliwiają konfigurowanie, aktualizowanie i utrzymanie właściwego czasu na wewnętrznym zegarze systemowym.

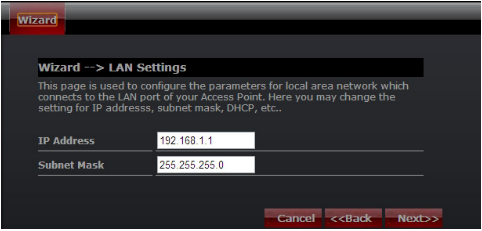


Time Zone Select: Wybierz odpowiednią strefę czasową z menu rozwijanego.

NTP Server: Wybierz Serwer NTP, z którego router ma pobierać informacje o aktualnym czasie.

Krok 3 - Ustawienia sieci LAN

Ustaw adres IP i maskę sieci dla interfejsu LAN.

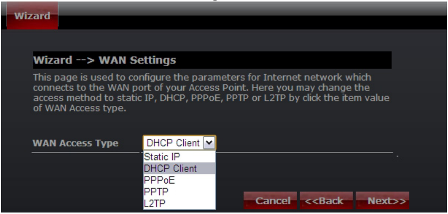


Krok 4 - Ustawienia WAN

Router obsługuje pięć trybów dostępu w sieci WAN, wybierz odpowiedni tryb w zależności od dostawcy usług internetowych.

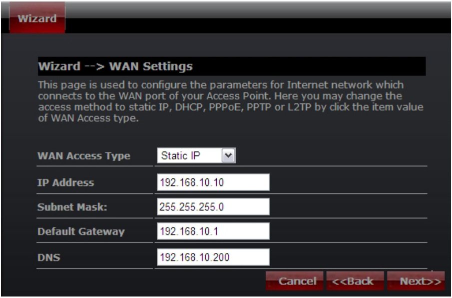
Tryb 1: Klient DHCP

Wybierz DHCP Clent w celu uzyskania adresu IP automatycznie od dostawcy Internetu (ISP). Tryb ten jest powszechnie stosowany w przypadku stosowania modemu kablowego.



Tryb 2: Static IP

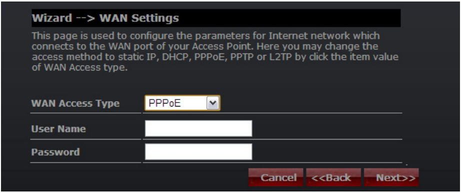
Wybierz opcję Static IP (stałego adresu IP), jeśli wszystkie informacje o adresie IP zostały dostarczone przez usługodawcę internetowego. Jeśli posiadasz te informacje wpisz je teraz: adres IP, maska podsieci, adres bramy oraz adres serwera DNS. Każdy adres IP wpisany w pola musi być wpisany w odpowiedniej formie – cztery liczby (od 0 do 255) oddzielone kropkami (X.X.X.X). Router nie przyjmie adresu IP, jeśli nie będzie wpisany w tym formacie.



Adres IP: Wpisz adres IP przypisany przez usługodawcę internetowego (Internet Service Provider). Maska podsieci: Wprowadź maskę podsieci przypisaną przez ISP. Default Gateway: Wpisz adres bramy przydzielony przez ISP.
DNS: Wpisz adres serwera DNS podany przez ISP.

Tryb 3: PPPoE

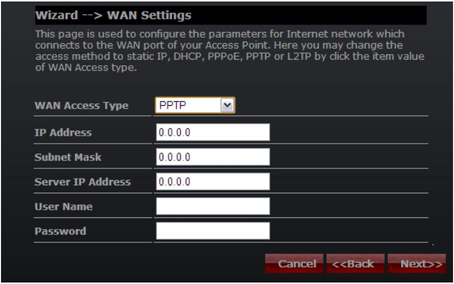
Wybierz PPPoE (Point to Point Protocol over Ethernet), jeśli usługodawca internetowy używa połączenia PPPoE. Twój dostawca zapewni Ci login i hasło.



Nazwa użytkownika: Wprowadź swoją nazwę użytkownika PPPoE.
Hasło: wpisz swoje hasło PPPoE.

Tryb 4: PPTP

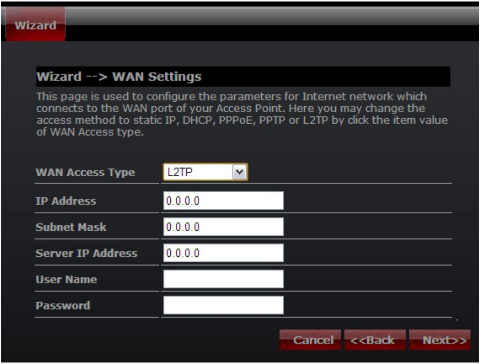
Wybierz PPTP (Point-to-Point-Tunneling Protocol), jeśli usługodawca internetowy korzysta z połączenia PPTP. Twój dostawca dostarczy Ci potrzebnych informacji (IP i adres IP serwera PPTP, nazwę użytkownika i hasło).



Adres IP: Wpisz adres IP.
Maska podsieci: Wprowadź maskę podsieci.
Adres IP serwera: Wprowadź adres IP serwera PPTP dostarczone przez ISP.
Nazwa użytkownika: Wprowadź swoją nazwę użytkownika PPTP.
Hasło: Wprowadź hasło PPTP.

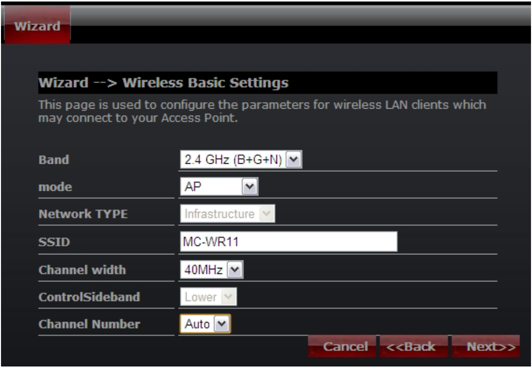
Tryb 5: L2TP

Wybierz L2TP (Layer 2 Tunneling Protocol), jeśli usługodawca internetowy korzysta z tego połączenia. Dostawca powinien dostarczyć Ci login i hasło oraz wszystkie potrzebne informacje.



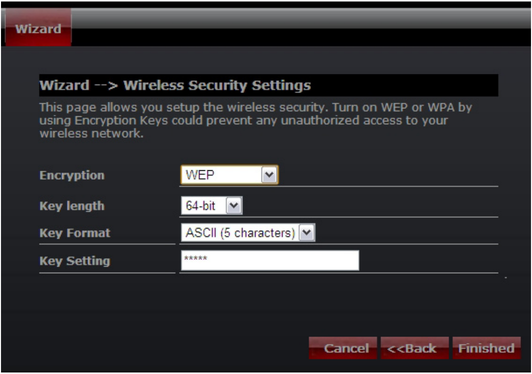
IP Address: Wpisz adres IP.
Subnet Mask: Wprowadź maskę podsieci.
Server IP Address: Wprowadź adres IP serwera PPTP dostarczone przez ISP.
User Name: Wprowadź swoją nazwę użytkownika PPTP.
Password: Wprowadź hasło PPTP.

Krok 5. Ustawienia sieci bezprzewodowej (WLAN)
Interfejs bezprzewodowy: Jeśli nie chcesz korzystać z bezprzewodowego, usuń zaznaczenie pola wyboru, aby wyłączyć wszystkie połączenia bezprzewodowe.



Band: Obsługa 802.11b, 802.11g, 802.11n oraz trybu mieszanego. Wybierz swoje pasma w zależności od tego jakich standardów używają urządzenia, które będą łączyć się z routerem.
Tryb: Obsługiwane są tryby – Punkt dostępowy (AP), Klient (Clent), WDS oraz AP + WDS.
Typ sieci: Ten typ jest ważny tylko w trybie klienta.
SSID: Service Set Identifier – identyfikator sieci bezprzewodowej.
szerokość kanału: Wybierz 40MHz jeśli używasz 802.11n lub 802.11n trybie mieszanym, w przeciwnym razie wartość domyślna to 20MHz.
ControlSideband: Jest ono ważne tylko po wybraniu szerokości kanału 40MHz.
Channel Number: Wskazuje ustawienie kanału na routerze. Domyślnie jest ustawiony na kanał 6.

Krok 5. Ustawienia zabezpieczeń sieci bezprzewodowej (WLAN)
Zabezpiecz sieć bezprzewodową poprzez włączenie funkcji zabezpieczeń WPA lub WEP na routerze. W tej sekcji możesz ustawić tryb zabezpieczeń WEP i WPA, WPA2 lub tryb mieszany.
Poniższy rysunek pokazuje, jak ustawić zabezpieczenia WEP.



Długość klucza: WEP obsługuje 64-bitowy klucz zabezpieczeń lub 128-bitowe.
Key Format: Użytkownik może wpisać klucz w formacie ASCII lub Hex.
Key Setting: Wprowadź klucz zgodny z wybranym formatem.

Klucze są używane do szyfrowania danych przesyłanych w sieci bezprzewodowej. Wpisz klucz spełniający następujące kryteria:

• 64-bit: minimalna długość klucza:

5 znaków (dla kluczy składających się ze znaków “A-F”, “a-f”)
10 znaków (dla kluczy składających się z cyfr 0-9)
Zalecane jest używanie kluczy składających się z małych i wielkich liter oraz cyfr – na przykład: “012345aEfG”

• 128-bit: minimalna długość klucza:
13 znaków (dla kluczy składających się ze znaków “A-F”, “a-f”)
26 znaków (dla kluczy składających się z cyfr 0-9)
Zalecane jest używanie kluczy składających się z małych i wielkich liter oraz cyfr – na przykład: “01234567890123456789aBcDEf”
Poniższy rysunek przedstawia, jak ustawić zabezpieczenia WPA-PSK, można wybrać WPA (TKIP), WPA2 (AES) lub tryb mieszany.



Pre-Shared Key Format: Określ format klucza, hasła lub hex.
Pre-Shared Key: Wprowadź klucz zgodny z wybranym formatem.

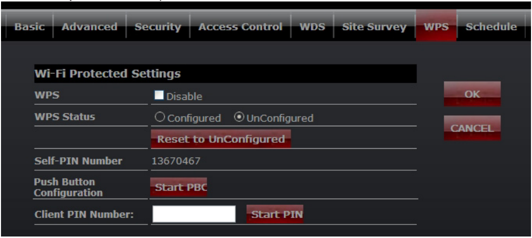
Klucze są używane do szyfrowania danych przesyłanych w sieci bezprzewodowej. Wpisz klucz spełniający następujące kryteria:
• 64-bit: minimalna długość klucza:
5 znaków (dla kluczy składających się ze znaków “A-F”, “a-f”)
10 znaków (dla kluczy składających się z cyfr 0-9)
Zalecane jest używanie kluczy składających się z małych i wielkich liter oraz cyfr – na przykład: “012345aEfG”
•128-bit: minimalna długość klucza:
13 znaków (dla kluczy składających się ze znaków “A-F”, “a-f”)
26 znaków (dla kluczy składających się z cyfr 0-9)
Zalecane jest używanie kluczy składających się z małych i wielkich liter oraz cyfr – na przykład: “01234567890123456789aBcDEf”

Rozdział 4 - Advanced Setup

4.1 Ustawienia zaawansowane sieci bezprzewodowej (WLAN)

4.1.1 WPS

WPS został stworzony w celu ułatwienia konfiguracji sieci bezprzewodowej (Wi-Fi). Ten router obsługuje funkcję WPS w trybie punktu dostępowego (AP), AP + WDS, Infrastructure-Client oraz trybu powielania sygnału (Universal Repeater Mode).

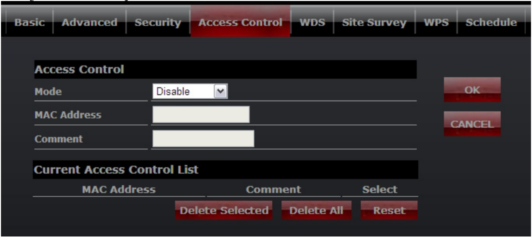


WPS: Zaznaczenie tego pola wyboru „Disable” i kliknięcie „OK” spowoduje wyłączenie funkcji WPS. Funkcja WPS jest domyślnie włączona.
Status WPS: Domyślnie szyfrowanie sieci bezprzewodowej jest wyłączone i WPS jest nieskonfigurowany. Niektóre usługi, takie jak Vista WCN mogą skonfigurować punkt dostępowy routera. W przeciwnym razie, jeśli WPS Status jest ustawiony na „Configured” oznacza to, że router ma skonfigurowane parametry zabezpieczeń.
Self-PIN Number: Numer PIN punktu dostępowego.
Start PBC: Kliknięcie tego przycisku rozpocznie sesję konfiguracji WPS. Jeżeli stacja chce się połączyć z AP, należy kliknąć jego przycisk PBC w przeciągu dwóch minut. W trakcie trwania sesji dioda WPS będzie migać.

Uwaga: Ten router posiada również przycisk sprzętowy WPS (z tyłu obudowy) - ten sam przycisk, który służy do resetowania urządzenia. Po naciśnięciu i przytrzymaniu tego przycisku, przez mniej niż dwie sekundy, roz-

poczęta zostanie sesja WPS, w tym czasie migać będzie dioda WPS. Inne urządzenie sieciowe może połączyć się w tym czasie z routerem przez rozpoczęcie sesji WPS za pośrednictwem oprogramowania lub sprzętowego przycisku WPS. Dodatkowa uwaga – przytrzymanie przycisku WPS/Reset od 2 do 5 sekund spowoduje ponowne uruchomienie routera; dłużej niż 5 sekund – przywrócone zostaną ustawienia fabryczne.
Client PIN number: Długość PIN jest ograniczona do czterech lub ośmiu cyfr. Jeśli punkt dostępowy i klient mają wpisany ten sam numer PIN i uruchomioną sesję WPS (poprzez kliknięcie przycisku „Start PIN") w przeciągu dwóch minut – powinny nawiązać połączenie ustawić klucz zabezpieczeń sieci bezprzewodowej.

4.1.2 Kontrola dostępu
Funkcja filtrowania w oparciu o adres MAC pozwala na kontrolę dostępu urządzeń sieciowych do routera.



Mode (Tryb): Jeśli wybierzesz „**Allow listed**", z routerem będą mogły połączyć się tylko te urządzenia, których adresy MAC sieci bezprzewodowej znajdują się na liście kontroli dostępu. Jeśli wybrana jest opcja „**Deny listed**" urządzenia, których adresy znajdują się na liście nie będą mogły łączyć się z routerem. MAC Address ma format 001122334455.

4.1.3 WDS (Wireless Distribution System)
WDS pozawala na powiększanie zasięgu sieci bezprzewodowej przez przekazywanie sygnału innego punktu dostępowego. Aby to zrobić, najpierw należy ustawić tryb pracy sieci bezprzewodowej na WDS AP lub AP + WDS, a

następnie włączyć funkcję WDS i podać adres MAC innego punktu dostępowego, z którym router ma się komunikować. WDS obsługuje szyfrowanie WEP i tryb zabezpieczeń WPA. Oczywiście w celu prawidłowej pracy punktu dostępowego, musisz ustawić ten sam kanał i tryb zabezpieczeń co w źródłowym punkcie dostępowym, którego sygnał ma być przekazywany.



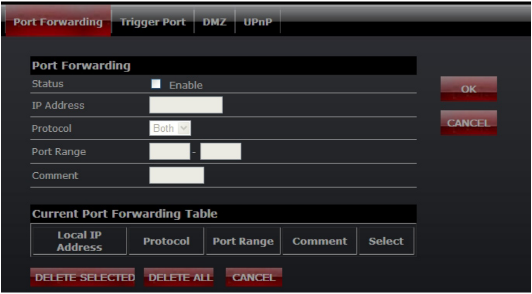
WDS: zaznacz to pole, aby włączyć funkcję WDS.
MAC Address (Adres MAC): wpisz adres MAC źródłowego punktu dostępowego.
Security (Zabezpieczenia): ustawienia zabezpieczeń WDS.
Encryption (Szyfrowanie): Możesz wybrać 64bits WEP, WEP 128bits, WPA (TKIP), WPA (AES).
WEP Key Format: Możesz wybrać, aby wybrać znaków ASCII lub znaków szesnastkowych (w zakresie „A-F", „a-f" i „0-9") do klucza WEP.
WEP Key: Ustaw klucz do szyfrowania danych
Pre-Shared Key Format: Możesz wybrać hasło lub HEX (64 znaków).
Pre-Shared Key: Wprowadź klucz zgodny z wybranym formatem.

4.2 Ustawienia usług

4.2.1 Przekierowanie portów (Port Forwarding)

Gdy router działa jako **serwer wirtualny** (Virtual Server), pozwala zdalnym użytkownikom na dostęp do usług takich jak serwer WWW czy FTP wewnątrz sieci lokalnej poprzez publiczny adres IP, automatycznie przekierowywany

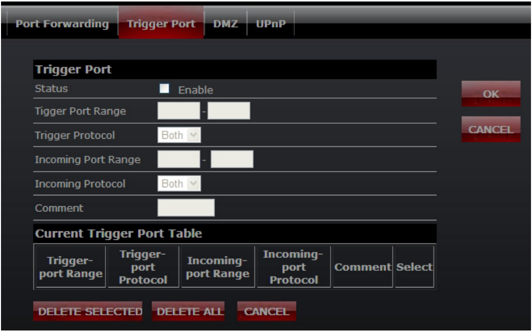
na serwery lokalne posiadające prywatny adres IP. Innymi słowy, w zależności od usługi (numeru portu TCP / UDP), router przekierowuje zewnętrzne żądanie usługi do odpowiedniego serwera wewnątrz sieci lokalnej.



Status: Zaznacz pole „Enable" by aktywować funkcję **przekierowania portów** (Port Forwarding).
Adres IP: Adres, na który ma być przekierowane zapytanie od zewnętrznego użytkownika.
Protokół i Port Rangę: pakiet z tego protokołu i portu, zostanie przekierowany na wskazany adres IP.
Comment: Możesz dodać komentarz do tej pozycji.
Tabela Skonfigurowanych przekierowań: Tabela przedstawia wszystkie skonfigurowane zestawienia adresów i portów. Możesz usunąć jedną lub wszystkie pozycje.

4.2.2 Wyzwalanie portów (Trigger Port)

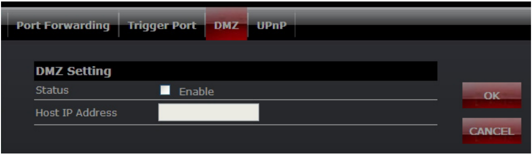
Niektóre aplikacje - takie jak gry internetowe, konferencje wideo itp. - wymagają wielu połączeń. Niektóre z tych aplikacji nie mogą działać ze zwykłym serwerem NAT. Funkcja wyzwalania portów pozwala routerowi na otwarcie portów dla przychodzącego ruchu i zamknięcie ich, gdy nie są używane. Gdy zostanie wysłane zapytanie router będzie oczekiwał odpowiedzi od zdalnego serwera i odpowiedni port zostanie otwarty.



Status: Włączenie i wyłączanie funkcji.
Trigger Port Range: Zakres portów monitorowanych przez router dla ruchu wychodzącego. Połączenie wychodzące za pośrednictwem portu z tego zakresu wyzwoli ustanawianie reguł .
Trigger Protocol: Protokół używany przez Port Trigger: TCP, UDP lub oba (Both).
Incoming Port Range: Zakres portów lub port używany przez system podczas odpowiadania na żądanie wychodzące. Odpowiedzi przy użyciu jednego z tych portów zostaną przekazane do komputera, który wywołał regułę.
Incoming Protocol: Protokół używany do odpowiedzi TCP, UDP, lub oba (Both).
Comment (Komentarz): Można dodać opis lub komentarz do tej pozycji.

4.2.3 Strefa zdemilitaryzowana (DMZ)

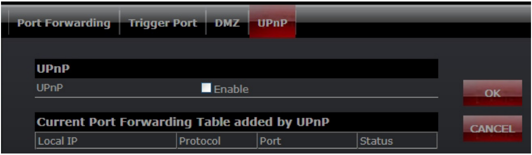
Jeśli jakiś program zainstalowany na komputerze w sieci lokalnej, nie działa właściwie zza NAT lub/i Firewalla lub po skonfigurowaniu Port Forwarding, można otworzyć nieograniczony połączenie z Internetem w dwóch kierunkach.



Status: Włączenie i wyłączanie funkcji.
Host IP Address: Wpisz adres IP hosta DMZ – używanie tej funkcji może narazić ten komputer na wiele zagrożeń.

4.2.4 Universal Plug and Play (UPnP)

Funkcja UPnP pozwala urządzeniom uzyskać dostęp do lokalnych zasobów komputera lub innych urządzeń. Urządzenia UPnP mogą być automatycznie wykrywane przez usługi UPnP w sieci lokalnej.



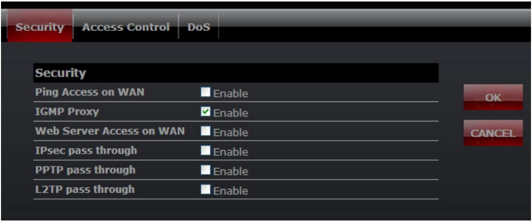
UPnP: Włączenie i wyłączanie funkcji.
Uwaga: Wymieniony jest również przekazywany port dodany przez usługę UpnP.

4.3 Ustawienia zabezpieczeń

Router zapewnia szeroką ochronę dzięki Firewallowi przez ograniczenie parametrów połączenia w celu ograniczenia ryzyka włamania i obrony przed szeroką gamą najczęściej spotykanych ataków hakerów.

4.3.1 Bezpieczeństwo

Zapora Firewall będzie blokować lub przepuszczać usługi zgodnie z następującymi ustawieniami.



Ping Access on WAN: Czy zezwolić lub zablokować usługę ping z interfejsu WAN.

IGMP Proxy: Prosty, dynamiczny Demon Multicast Routing używający tylko sygnalizacji IGMP. Jest on przeznaczony do łatwego przekazywania ruchu Multicast pomiędzy sieciami.

Web Server Access on WAN: Czy pozwolić na dostęp do serwera WWW z interfejsu WAN.

VPN pass through: Przepuszczanie połączeń Virtual Private Network (VPN).

4.3.2 Kontrola dostępu

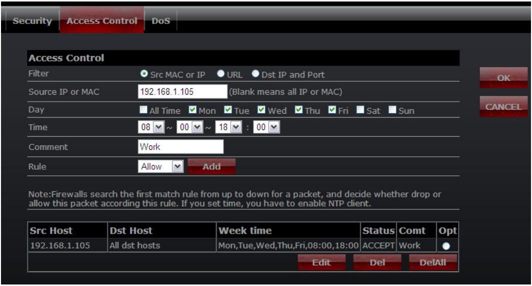
W tej sekcji można skonfigurować kilka zasad, na przykład filtrowanie adresów MAC, filtrowanie IP, filtr adresów URL, filtrowanie Portów. Można również dodać dodatkowe reguły odnoszące się do daty i czasu, ale należy wcześniej włączyć klienta NTP.

Uwaga 1: Kiedy pakiet dotrze do routera, zapora Firewall przeszuka tabelę zasad i zatrzyma się, jeśli znajdzie pasującą do niego regułę. Następnie pakiet będzie przepuszczony lub odrzucony zgodnie z regułą. Jeśli nie ma odpowiedniej reguły, Firewall przepuści pakiet.

Uwaga 2: Kliknij przycisk „Dodaj", aby dodać regułę do tabeli i kliknij „OK" zastosuje zapisane reguły. Możesz również edytować lub kasować wcześniej dodane zasady.

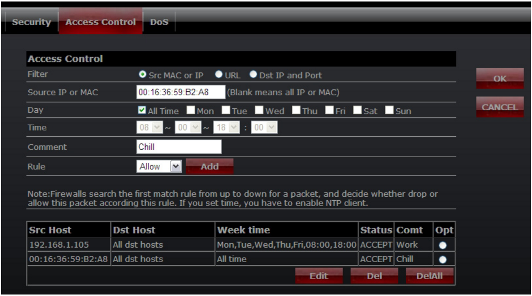
1. Filtr IP

Przepuść lub zablokuj połączenia komputerów w oparciu o ich adresy IP.



2. Filtrowanie adresów MAC

Przepuść lub zablokuj połączenia komputerów w oparciu o ich adresy MAC.

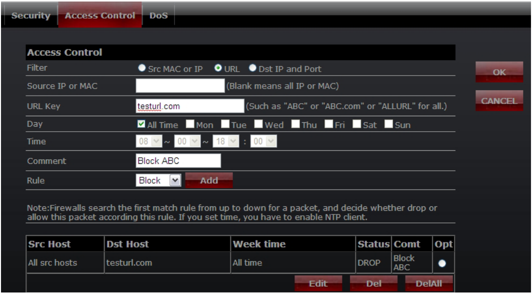


3. Filtr URL

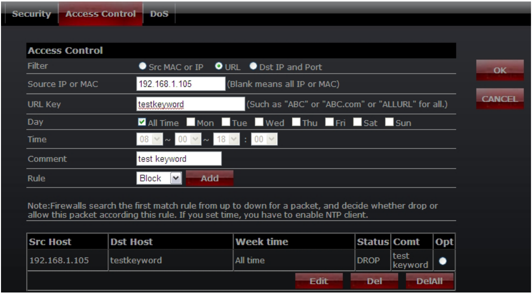
Możesz blokować niektóre adresy URL według słów kluczowych. Jeśli pole Source IP lub MAC jest puste, oznacza to, że wszystkie komputery nie mają

dostępu do tego adresu URL, w przeciwnym razie reguła jest ważna tylko dla jednego komputera z tym adresem IP lub MAC.

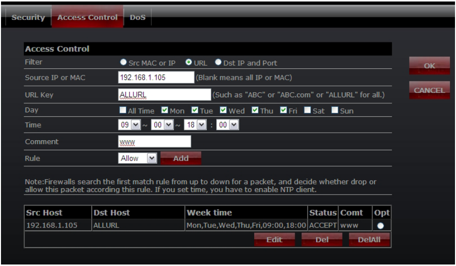
Przykład 1: Blokuj adres „testurl.com” dla wszystkich komputerów.



Przykład 2: Blokuj dostęp do adresów zawierających słowo kluczowe „test-keyword” dla jednego komputera o adresie IP 192.168.1.105.



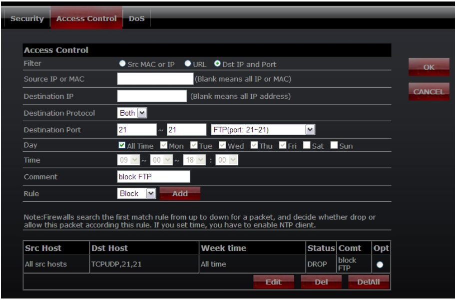
Przykład 3: Blokuj dostęp do wszystkich adresów URL dla jednego komputera o adresie IP 192.168.1.105 w dni robocze od 09:00 do 18:00.



4. Filtrowanie portów.

Można ograniczyć dostęp niektórym lub wszystkim komputerom dostęp do adresu IP i portu docelowego.

Przykład 1: Blokowanie dostępu do portu 21.

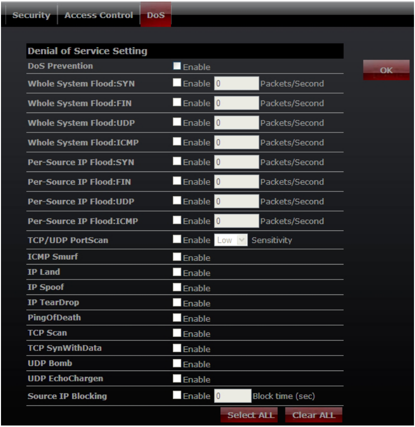


Przykład 2: Blokowanie jednemu komputerowi (o adresie IP 192.168.1.101) dostępu do portu 21.



4.3.3 Blokowanie ataków typu Denial of Service (DoS)

Ta strona zawiera ustawienia blokowania ataków DoS.



4.4 Konfiguracja QoS

QoS pozwala zwiększyć wydajność np. w grach przez nadawanie priorytetu aplikacjom. Domyślnie kontrola pasma jest wyłączona, a pierwszeństwo aplikacji nie jest automatycznie klasyfikowane.

W celu skonfigurowania Qos, wykonaj następujące kroki:

Włącz QoS.

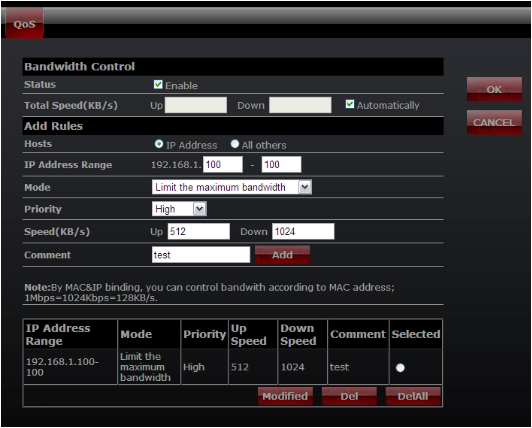
Wpisz wartość całkowitej prędkości połączenia lub pozwól na automatyczne wykrycie tych wartości.

Wpisz adres(y) IP użytkownika(ów) dla których ma być stosowana reguła.

Określ w jaki sposób ma być limitowana prędkość połączenia - minimalna lub maksymalna przepustowość / priorytet: wysoki (High) lub niski (Low).

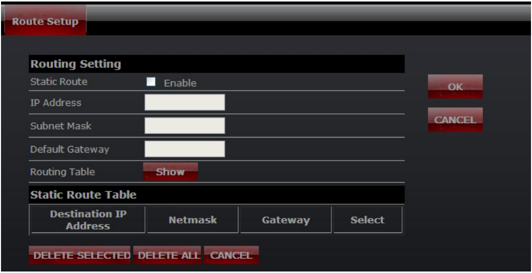
Kliknij przycisk „Add", aby dodać ten element do tabeli

Kliknij przycisk OK, aby zastosować zestaw reguł.



4.5 Router Setup

Statyczna trasa to z góry określony szlak, którym pakiety danych muszą podróżować by dotrzeć do określonego hosta lub sieci.

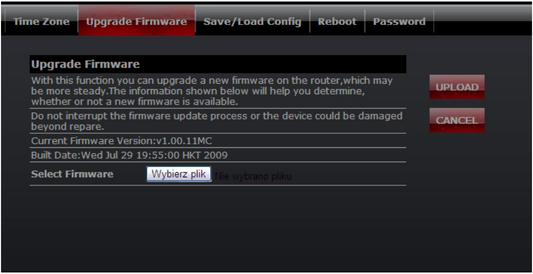


Static Route: Zaznacz pole „Enable", aby umożliwić ustawienie trasy statycznej.
Adres IP: Adres IP docelowej sieci lub hosta.
Subnet Mask: Docelowa maska podsieci .
Default Gateway: Adres IP Bramy, czyli routera lub komputera, do którego pakiet ma być wysłany. Adres ten musi być w tym samy segmencie sieci WAN lub LAN.
Tabela routingu: Kliknięcie tego przycisku umożliwia wyświetlenie tablicy routingu systemu.
Tabela Static Routing: Zawiera elementy tabeli routingu statycznego. Można usunąć jeden lub wszystkie elementy.

4.6 System

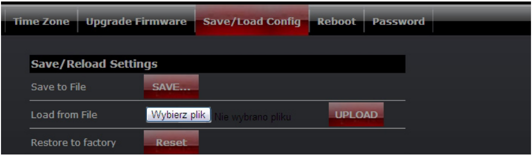
4.6.1 Aktualizacja oprogramowania

Na tej stronie można uaktualnić oprogramowanie.



4.6.2 Zapisz / Wczytaj ustawienia routera

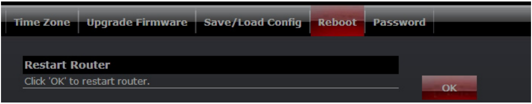
Można wykonać kopię zapasową lub przywrócić konfigurację systemu na tej stronie.



Save to File (Zapisz do pliku): Zapisz ustawienia routera na komputerze lokalnym.
Load from File (Załaduj z pliku): Przywracanie ustawień routera z zapisanego pliku.
Resotore factory (Przywróć ustawienia fabryczne): Przywracanie ustawień systemu do ustawień fabrycznych.

4.6.3 Ponowne uruchomienie (Reboot)

Urządzenie można ponownie uruchomić poprzez kliknięcie przycisku Reboot.



4.6.4 Hasło

Aby zapewnić bezpieczeństwo routera, użytkownik zostanie poproszony o podanie nazwy użytkownika i hasła przy próbie dostępu do panelu konfiguracyjnego routera. **Domyślna nazwa użytkownika i hasło: admin / admin**.

Ta strona pozwoli Ci zmienić nazwę użytkownika i hasło.



ENVIRONMENT PROTECTION:
This symbol on our product nameplates proves its compatibility with the EU Directive2002/96 concerning proper disposal of waste electric and electronic equipment (WEEE). By using the appropriate disposal systems you prevent the potential negative consequences of wrong product take-back that can pose risks to the environment and human health. The symbol indicates that this product must not be disposed of with your other waste. You must hand it over to a designated collection point for the recycling of electrical and electronic equipment waste. The disposal of the product should obey all the specific Community waste management legislations. Contact your local city office, your waste disposal service or the place of purchase for more information on the collection.
Weight of the device: ~324g

OCHRONA ŚRODOWISKA:
Niniejsze urządzenie oznakowane jest zgodnie z dyrektywą Unii Europejskiej 2002/96/UE dotyczącą utylizacji urządzeń elektrycznych i elektronicznych (WEEE). Zapewniając prawidłowe usuwanie tego produktu, zapobiegasz potencjalnym negatywnym konsekwencjom dla środowiska naturalnego i zdrowia ludzkiego, które mogą zostać zagrożone z powodu niewłaściwego sposobu usuwania tego produktu. Symbol umieszczony na produkcie wskazuje, że nie można traktować go na równi z innymi odpadami z gospodarstwa domowego. Należy oddać go do punktu zbiórki zajmującego się recyklingiem urządzeń elektrycznych i elektronicznych. Usuwanie urządzenia musi odbywać się zgodnie z lokalnie obowiązującymi przepisami ochrony środowiska dotyczącymi usuwania odpadów. Szczegółowe informacje dotyczące usuwania, odzysku i recyklingu niniejszego produktu można uzyskać w urzędzie miejskim, zakładzie oczyszczania lub sklepie, w którym nabyłeś niniejszy produkt.
Masa sprzętu: ~324g